

CLAIMS

Having thus described my invention, what I claim as new and desire to secure by Letters Patent is as follows:

- 1 1. A method enabling a user of a computing system to generate a secret value
2 from answers to questions previously created by the user, said method comprising
3 the steps of:
4 displaying the questions previously created by the user;
5 prompting the user to select a first portion of the displayed questions and
6 provide a first set of answers to the selected first portion of questions;
7 attempting to generate said secret value from a portion of the first set of
8 answers and possibly other information;
9 if said secret value cannot be generated from at least a portion of the first
10 set of answers and possibly other information, prompting the user to select a
11 second portion of the displayed questions and provide a second set of answers to
12 the selected second portion of questions; and
13 attempting to generate said secret value from a portion of said first and
14 second sets of answers and possibly other information.

- 1 2. The method of claim 1, wherein there are n questions previously created by the
2 user, and the user is prompted to select as said first portion at least m questions to
3 answer but, at the user's option, can select k questions to answer, where
4 $0 < m \leq k \leq n$ and the set of k questions consists of a first subset of m questions
5 and an optional subset of k_1 questions ($k_1 = k - m$).

- 1 3. The method of claim 2, wherein there are n questions previously created by the
2 user, and the user is prompted to select as said second portion a third set k_2 of the
3 $n - m - k_1$ additional unanswered questions, where $0 < k_2 \leq n - m - k_1$ and k_2 is a
4 variable value determined by the PE user.

- 1 4. The method of claim 3, wherein the PE user is allowed to repeat the step of
2 selecting as said second portion a third set k_2 of the unanswered questions until
3 one of the following conditions is met: (1) the PE user is successfully
4 authenticated, (2) the PE user chooses to discontinue, or (3) the PE user fails to
5 be authenticated after answering all n questions.

- 1 5. The method of claim 3, wherein the at least one of the values k_1 and k_2 is a
2 constant.

- 1 6. The method of claim 3, wherein $n=9$, $m=5$, and $k_1=0$.

- 1 7. The method of claim 6, wherein k_2 is a variable value of 1, 2, 3, or 4 selected by
2 the PE user.

- 1 8. The method of claim 1, wherein there are n questions previously created by the
2 user, and the user is prompted to select as said first portion m questions to
3 answer, where $0 < m < n$, and the user is prompted to select as said second
4 portion 1 to $n-m$ as said second portion.

- 1 9. The method of claim 1, wherein there are n questions previously created by the
2 user, and the user is prompted to select as said first portion at least m questions to
3 answer but, at the user's option, can select k questions to answer, where
4 $0 < m \leq k \leq n$ and the set of k questions consists of a first subset of m questions
5 and an optional subset of k_1 questions ($k_1 = k - m$), and wherein the PE user is
6 authenticated of m questions and answers in a predetermined way from among the
7 questions and answers specified by the PE user.

- 1 10. The method of claim 9, wherein the PE user is allowed to repeat the step of
2 selecting as said second portion a third set k_2 of the unanswered questions until

3 one of the following conditions is met: (1) the PE user is successfully
 4 authenticated, (2) the PE user chooses to discontinue, or (3) the PE user fails to
 5 be authenticated after answering all n questions.

1 11. The method of claim 10, wherein the PE user is allowed to repeat the step of
 2 selecting as said second portion a third set k_2 of the unanswered questions until
 3 one of the following conditions is met: (1) the PE user is successfully
 4 authenticated, (2) the PE user chooses to discontinue, or (3) the PE user fails to
 5 be authenticated after answering all n questions.

1 12. The method of claim 11, wherein the at least one of the values k_1 and k_2 is a
 2 constant.

1 13. The method of claim 11, wherein $n=9$, $m=5$, and $k_1=0$.

1 14. The method of claim 13, wherein k_2 is a variable value of 1, 2, 3, or 4 selected
 2 by the PE user.

1 15. The method of claim 1, wherein if the PE user fails to be authenticated in
 2 successive invocations the step of attempting to generate said secret value, the PE
 3 user is required to correctly answer a number of questions greater than m .

1 16. The method of claim 15, wherein if the PE user fails to be authenticated in
 2 two or three successive invocations of the step of attempting to generate said
 3 secret value, the PE user is required to correctly answer $m+1$ questions.

1 17. The method of claim 16, wherein if the PE user fails to be authenticated in
 2 four or more successive invocations of the step of attempting to generate said
 3 secret value, the PE user is required to correctly answer $m+2$ questions.

1 18. The method of claim 1, further comprising the steps of:
2 authenticating the user upon generating the secret value; and
3 displaying incorrect answers to the user who has been successfully
4 authenticated.

1 19. A method enabling a user of a computing system to generate a secret value
2 from answers to questions previously created by the user, said method comprising
3 the steps of:
4 displaying the questions previously created by the user;
5 prompting the user to select a first portion of the displayed questions and
6 provide a first set of answers to the selected first portion of questions;
7 attempting to generate said secret value from a portion of the first set of
8 answers and possibly other information;
9 prompting the user to select a second portion of the displayed questions
10 and provide a second set of answers to the selected second portion of questions;
11 attempting to generate said secret value from a portion of said first and
12 second sets of answers and possibly other information;
13 prompting the user to select a third portion of the displayed questions and
14 provide a third set of answers to the selected third portion of questions, if said
15 secret value cannot be generated from at least a portion of the first and second
16 sets of answers and possibly other information; and
17 attempting to generate said secret value from a portion of said first,
18 second, and third sets of answers and possibly other information, if said secret
19 value cannot be generated from at least a portion of the first set of answers and
20 possibly other information.

1 20. A method enabling a user of a computing system to generate a secret value
2 from answers to questions previously created by the user, said method comprising
3 the steps of:
4 displaying the questions previously created by the user;

5 prompting the user to select at least a portion of the displayed questions
 6 and provide answers to the selected portion of questions;
 7 attempting to generate said secret value from a first sub-portion of the
 8 provided answers and possibly other information; and
 9 if said secret value cannot be generated from said first sub-portion of the
 10 provided answers and possibly other information, attempting to generate said
 11 secret value from a second sub-portion of the provided answers.

1 21. The method of claim 20, wherein the second sub-portion of the provided
 2 answers has a greater number of answers than the first sub-portion of the provided
 3 answers.

1 22. The method of claim 20, wherein the second sub-portion of the provided
 2 answers contains some of the answers of the first sub-portion.

1 23. The method of claim 20, wherein the second sub-portion of the provided
 2 answers contains all of the answers of the first sub-portion.

1 24. The method of claim 20, wherein the second sub-portion of the provided
 2 answers contains none of the answers of the first sub-portion.

1 25. A method enabling a user of a computing system to generate a secret value
 2 from answers to questions previously created by the user, said method comprising
 3 the steps of:

4 displaying the questions previously created by the user;
 5 prompting the user to select a first portion of the displayed questions and
 6 provide a first set of answers to the selected first portion of questions;
 7 prompting the user to select a second portion of the displayed questions
 8 and provide a second set of answers to the selected second portion of questions;
 9 attempting to generate said secret value from a portion of the first set of

10 answers and possibly other information; and
 11 if said secret value cannot be generated from at least a portion of the first
 12 set of answers and possibly other information, attempting to generate said secret
 13 value from a portion of the first and second sets of answers and possibly other
 14 information.

1 26. The method of claim 25, wherein if said secret value cannot be generated from
 2 at least a portion of the first and second sets of answers and possibly other
 3 information, further comprising the step of prompting the user to select a third
 4 portion of the displayed questions and provide a third set of answers to the
 5 selected third portion of questions.

1 27. A computing system enabling a user to generate a secret value from answers
 2 to questions previously created by the user, said computing system comprising:
 3 a user client computer, a controller computer and an authentication server
 4 computer;
 5 a network connecting said user computer, said controller computer and
 6 said authentication server computer;
 7 said controller computer downloading a client applet to said user client
 8 computer to begin an authentication session;
 9 said user client computer executing the client applet to display the
 10 questions previously created by the user and prompt the user to select a first
 11 portion of the displayed questions and provide a first set of answers to the
 12 selected first portion of questions;
 13 said authentication server computer attempting to generate said secret
 14 value from a portion of the first set of answers and possibly other information;
 15 said user client computer responding to said authentication server
 16 computer and prompting the user to select a second portion of the displayed
 17 questions and provide a second set of answers to the selected second portion of
 18 the questions if said secret value cannot be generated from at least a portion of the

19 first set of answers and possibly other information; and
20 said authentication server computer attempting to generate said secret
21 value from a portion of said first and second sets of answers and possibly other
22 information.

1 28. The computing system of claim 27, further comprising a repository of
2 downloadable client applets attached to the controller computer, the client applets
3 being downloadable to the user client computer and used for both creating the
4 secret value from answers supplied by the user when originally creating the
5 questions and, later, generating the secret value from answers provided by the
6 user to subsets of the previously created questions.

1 29. The computing system of claim 27, further comprising a central database
2 maintained by the authentication server computer, said central database containing
3 information created by users which can be subsequently accessed by the controller
4 server computer on behalf of the user.